SOLUTION BRIEF

# Evolving the NIST Cybersecurity Framework

## Tailor the framework to meet modern challenges

### CHALLENGE

- Identifying valuable risk insights and turning them into actionable protective measures remains challenging.
- Data is now stored everywhere and accessed from anywhere, and visibility remains fragmented.
- Too many alerts make it difficult to respond and recover, especially with manual processes.

### SOLUTION

- Forcepoint's risk-adaptive approach to security integrates best-in-class products with behavioral profiling, for near real-time risk insights and automated remediation to better protect federal users and data.
- Automation creates efficiencies for best use of resources to focus on ongoing needs.

### BENEFITS

- Automate policy enforcement to dynamically respond to changes in risk within an agency.
- Eliminate the need for a single, static data protection policy set.
- Allow for government agencies to achieve maximum data protection while preparing for evolving security requirements.

**In response to Executive Order 13636 on strengthening the cybersecurity of federal networks and critical infrastructure, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (FICIC) in February 2014 and revised it in 2018. The framework provides guidance for organizations looking to bolster their cybersecurity defenses.**

The NIST Framework provides a common language for understanding, managing, and expressing cybersecurity risk. That common language is used to help identify and prioritize actions for reducing risk and is a tool for aligning policy and technological approaches to risk management.

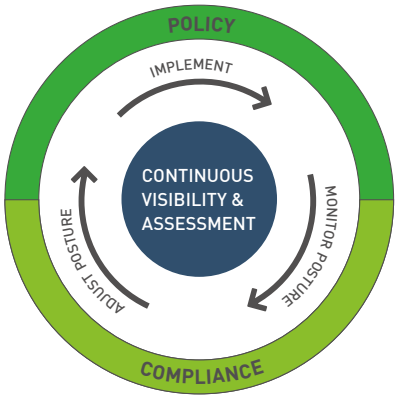
The Framework functions organize basic cybersecurity activities at their highest level. These functions—Identify, Protect, Detect, Respond, and Recover—aid in expressing management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

NIST's Cybersecurity Framework outlines how the functions are not intended to be a serial path or lead to a static desired end state. Rather, the functions are meant to be performed concurrently and continuously to form an operational culture that addresses dynamic cybersecurity risk.

## PRIORITIZING NIST CYBERSECURITY REMEDIATION

Digital transformation, cloud, and mobility have driven information technology to an inflection point and security architectures to a breaking point. Traditional approaches to data protection leave government systems drowning in alarms and alerts, while security organizations are struggling to review and triage security content, adjust system policies, and remediate risk. Today, security teams are spending too much time responding to alerts and security events and far too little on concurrently and continuously focusing on post-breach planning and recovery.

Instead of trying to extend the traditional, event-centric approach by adding more layers or crunching more data, we need a paradigm shift that places human behavior at the center of cybersecurity. Cybersecurity professionals need to focus on two constants—people and data—and where the two come together.




**THE NIST CYBERSECURITY FRAMEWORK REQUIRES CONTINUOUS MONITORING**

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

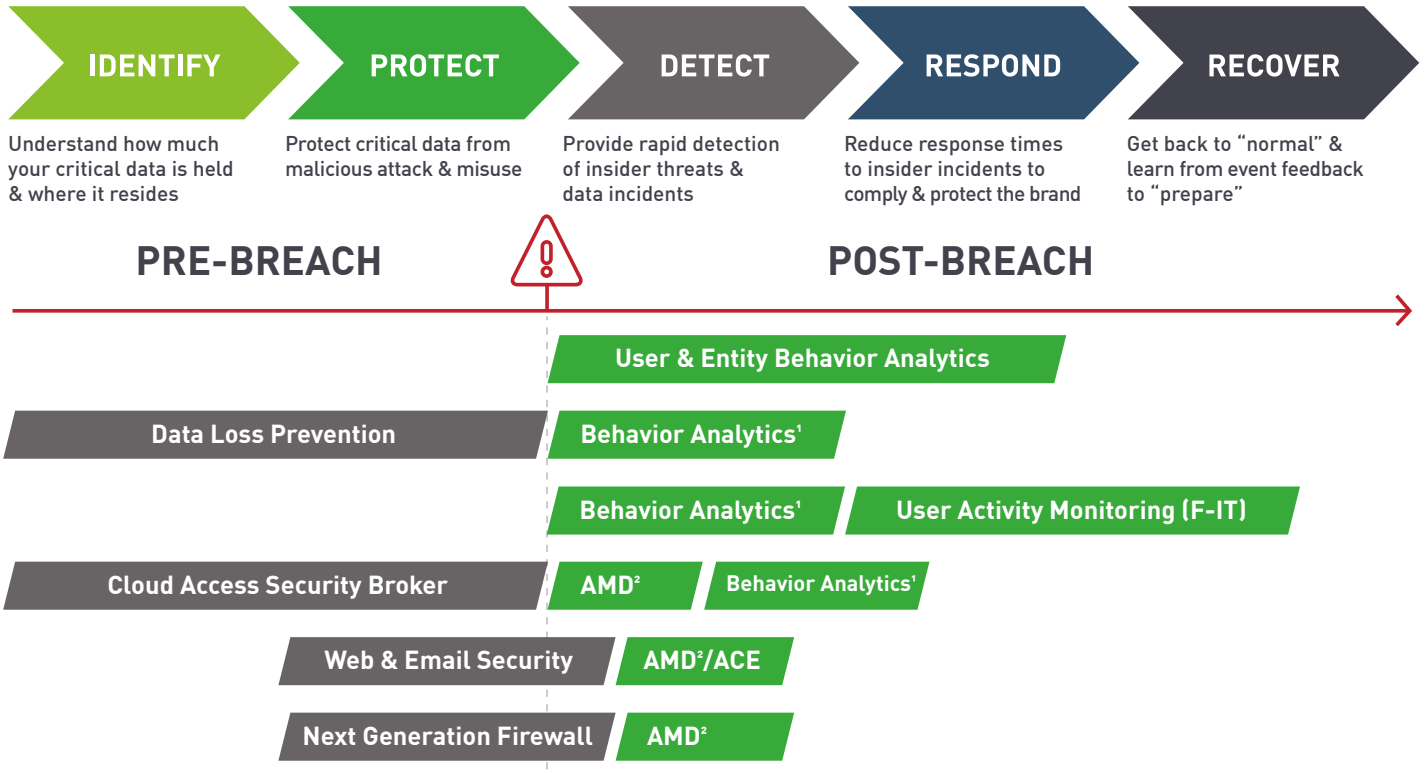
## RISK-ADAPTIVE SECURITY IS A NEW APPROACH IN FULL ALIGNMENT WITH THE NIST CYBERSECURITY FRAMEWORK

Risk-adaptive security leverages behavior analytics, unified policy, and orchestration to deliver dynamic security that adapts to users' real-time risk levels. Risk-adaptive security provides insight into user behavior and data flow to rapidly identify risk, automate policies, and reduce the quantity of alerts requiring investigation. With risk-adaptive security, agencies can protect users, data, and networks in real time and increase the efficacy of their security investments.

### Forcepoint's Human Point System Enables NIST Cybersecurity Framework:

- Capture interactions between users and data everywhere
- Generate a dynamic risk score by understanding context
- Respond automatically to compromised, accidental, and malicious behavior
- Gain efficiencies in investigation and operations through context, such as detailed timelines of events

## FORCEPOINT BRINGS TOGETHER A BROAD SET OF CAPABILITIES TO ADDRESS NIST REQUIREMENTS:




**Introducing Forcepoint's risk-adaptive security approach.** Now, there is a smarter way to safeguard sensitive networks and data, no matter where they reside or are accessed. Forcepoint's risk-adaptive security approach allows government agencies to identify high-risk activity and automate policies to protect data in near real time, providing the highest security with the greatest end-user productivity. Forcepoint's human-centric cybersecurity approach integrates best-in-class products with analytics and behavioral profiling, bringing agencies near real time risk insights and automated remediation to better protect government users' data, including Controlled Unclassified Information (CUI), wherever it resides, with solutions that maintain the integrity of the NIST's Cybersecurity Framework and enable a sustainable and continuous operational culture that addresses dynamic cybersecurity risk.

[1]Integrated Behavioural Analytics [2]Includes Advanced Malware Defense Module

**CONTACT**
**www.forcepoint.com/contact**